

JC20 Rec'd PCT/PTO 03 OCT 2005

DOCKET NO.: 278167US6PCT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF: Takashi KOIKE, et al.

SERIAL NO.: NEW U.S. PCT APPLICATION

FILED: HERewith

INTERNATIONAL APPLICATION NO.: PCT/JP04/04288

INTERNATIONAL FILING DATE: March 26, 2004

FOR: DIGITAL DATA STORAGE/REPRODUCTION METHOD AND DEVICE

**REQUEST FOR PRIORITY UNDER 35 U.S.C. 119  
AND THE INTERNATIONAL CONVENTION**Commissioner for Patents  
Alexandria, Virginia 22313


Sir:

In the matter of the above-identified application for patent, notice is hereby given that the applicant claims as priority:

**COUNTRY**  
Japan**APPLICATION NO**  
2003-107278**DAY/MONTH/YEAR**  
11 April 2003

Certified copies of the corresponding Convention application(s) were submitted to the International Bureau in PCT Application No. PCT/JP04/04288. Receipt of the certified copy(s) by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

Respectfully submitted,  
OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.



Gregory J. Maier  
Attorney of Record  
Registration No. 25,599  
Surinder Sachar  
Registration No. 34,423

Customer Number

**22850**

(703) 413-3000  
Fax No. (703) 413-2220  
(OSMMN 08/03)

26.3.2004

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

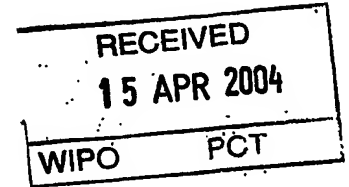
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年   4 月 1 1 日  
Date of Application:

出 願 番 号            特 願 2 0 0 3 - 1 0 7 2 7 8  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 3 - 1 0 7 2 7 8 ]

出   願   人            ソニー株式会社  
Applicant(s):

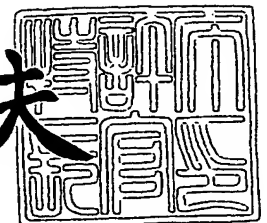


PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2 0 0 4 年   2 月 1 0 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0390212902

【提出日】 平成15年 4月11日

【あて先】 特許庁長官殿

【国際特許分類】 G11B 20/10

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 小池 隆

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 岩津 健

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社  
内

【氏名】 木村 学

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100091546

【弁理士】

【氏名又は名称】 佐藤 正美

【電話番号】 03-5386-1775

【手数料の表示】

【予納台帳番号】 048851

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9710846

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタルデータの保存方法および記録媒体

【特許請求の範囲】

【請求項 1】

内容が時間とともに変化するデジタルデータに対して、所定の時間ごとに所定の期間ずつ部分的に暗号化を行うとともに、

この暗号化部分の期間の上記所定の時間に対する割り合い、および上記暗号化部分の占める期間が、十分に小さくなるように上記暗号化を行い、

この暗号化のされたデジタルデータを保存する  
ようにしたデジタルデータの保存方法。

【請求項 2】

請求項 1 に記載のデジタルデータの保存方法において、

上記暗号化部分の位置を示す情報を、上記デジタルデータとともに保存する  
ようにしたデジタルデータの保存方法。

【請求項 3】

時間とともに変化する内容であって、所定の時間ごとに所定の期間ずつ部分的に暗号化が行われているとともに、

この暗号化部分の期間の上記所定の時間に対する割り合い、および上記暗号化部分の占める期間が、十分に小さくなるように上記暗号化が行われ、

この暗号化の行われたデジタルデータが記録されている  
ようにした記録媒体。

【請求項 4】

請求項 3 に記載の記録媒体において、

上記暗号化部分の位置を示す情報が、上記デジタルデータとともに記録されている

ように記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、オーディオ信号などのデジタルデータを保存するための技術に関する。

#### 【0002】

##### 【従来の技術】

デジタル処理やネットワーク技術の進展にともない、デジタルオーディオデータを放送やネットワークなどを通じてユーザに配信する技術が登場している。また、オーディオ機器として、配信されたデジタルオーディオデータを内蔵のHDDにいったん保存し、これを好きなときに取り出せるようにしたオーディオサーバも登場している（例えば、特許文献1参照）。また、オーディオサーバとして、デジタルオーディオデータを暗号化して保存し、認証を受けたときのみ、その暗号化されたデジタルオーディオデータを復号化して出力するようにしたものも考えられている（例えば、特許文献2参照）。

#### 【0003】

##### 【特許文献1】

特開 2003-30018 公報

#### 【0004】

##### 【特許文献2】

特開 2001-243705 公報

#### 【0005】

##### 【発明が解決しようとする課題】

ところで、オーディオサーバにおいては、そのサーバに組み込まれているソフトウェアにしたがった処理しか実行できないので、内蔵のHDDに保存されたデジタルオーディオデータをCD-Rなどにコピーすることはできない。しかし、オーディオサーバから内蔵のHDDを物理的に取り出してパーソナルコンピュータに接続すれば、そのHDDに保存されているデジタルオーディオデータを、他のHDDやCD-Rなどにコピーすることができ、著作権者の権利を守れなくなってしまう。

#### 【0006】

そこで、オーディオサーバにおいて、配信されたデジタルオーディオデータを

暗号化してから内蔵のHDDに取り込むことが考えられている。つまり、そのようにすれば、認証を受けたオーディオサーバにおいては、その暗号化されたデジタルオーディオデータを復号化することにより音楽などを正常に聴くことができる。

#### 【0007】

しかし、その内蔵のHDDを取り出してパーソナルコンピュータに接続しても、暗号化されたデジタルオーディオデータを復号化することはできないので、結果として、著作権を保護することができる。

#### 【0008】

ところが、家庭用のオーディオサーバは、概して使用しているCPUの処理能力が低いので、再生時、CPUによりデジタルオーディオデータを連続して復号化することができない。もちろん、CPUとして処理能力の高いものを使用すれば、あるいは復号化専用のICを設ければ、再生時、暗号化されたデジタルオーディオデータを連続して復号化することができるが、その場合には、サーバのコストが上昇してしまう。

#### 【0009】

この発明は、以上のような問題点を解決しようとするものである。

#### 【0010】

##### 【課題を解決するための手段】

この発明においては、例えば、

内容が時間とともに変化するデジタルデータに対して、所定の時間ごとに所定の期間ずつ部分的に暗号化を行うとともに、

この暗号化部分の期間の上記所定の時間に対する割り合い、および上記暗号化部分の占める期間が、十分に小さくなるように上記暗号化を行い、

この暗号化のされたデジタルデータを保存する

ようにしたデジタルデータの保存方法

とするものである。

したがって、デジタルデータを不正に再生した場合には、暗号化部分がノイズとして再生される。

## 【0011】

## 【発明の実施の形態】

図1は、この発明をオーディオサーバに適用した場合の一例を示すもので、符号10は各種のオーディオ信号のソース、符号20はオーディオ出力装置、符号30はこの発明によるオーディオサーバである。

## 【0012】

この場合、ソース10は、ネットワーク、CDプレーヤ、デジタル放送のチューナなどの信号源であり、オーディオ信号をデジタルデータ、つまり、デジタルオーディオデータの状態で提供するものである。また、出力装置20は、図示はしないが、D/Aコンバータ回路やスピーカなどを有し、ソース10あるいはオーディオサーバ30からデジタルオーディオデータが供給されると、そのデジタルオーディオデータを音響として出力するものである。

## 【0013】

さらに、オーディオサーバ30は、ユーザの指示にしたがって、ソース10から出力されるデジタルオーディオデータを保存し、あるいはその保存したデジタルオーディオデータを再生して出力装置20に出力するものである。このため、オーディオサーバ30はマイクロコンピュータにより構成されている。

## 【0014】

すなわち、オーディオサーバ30は、各種のプログラムを実行するCPU31と、ROM32と、ワークエリア用のRAM33と、ユーザインターフェイス34とを有し、これらがシステムバス39を通じて互いに接続されている。この場合、ROM32は、CPU31が実行する各種のプログラムが書き込まれている。また、ユーザインターフェイス34は、ユーザにより操作される各種の操作キー（操作スイッチ）、およびこの装置30の状態などを表示するディスプレイなどである。

## 【0015】

さらに、ソース10が入力インターフェイス35を通じてバス39に接続され、バス39が出力インターフェイス36を通じて出力装置20に接続される。また、大容量の保存手段として、例えばHDD38が設けられ、このHDD38が



HDC 37を通じてバス 39に接続されている。なお、HDD 38は、一般のパーソナルコンピュータなどにおいて使用されているHDDとすることができる。

#### 【0016】

また、バス 39には、暗号化回路 41、復号化回路 42および認証回路 43が接続される。ただし、この場合、暗号化回路 41、復号化回路 42および認証回路 43は、ソフトウェアにより構成されるものであり、すなわち、CPU 31がROM 32のプログラムを実行することにより実現されるものである。したがって、データ保存時の暗号化回路 41の暗号化処理およびデータ取り出し時の復号化回路 42の復号化処理は、そのデータの保存処理およびデータの取り出し処理と並行して実行されることになるので、CPU 31にとって負荷となる。なお、暗号化回路 41の暗号方式は、もとのデジタルデータとの相関がほとんどなくランダムノイズに近い暗号文データが作製される方式、例えばDES暗号化方式とされる。

#### 【0017】

さらに、認証回路 43は、例えば、出力装置 20をチェックし、これがあらかじめ設定されている正当な出力装置であるときのみ、出力装置 20へのデジタルオーディオデータの出力を許可するためのものである。

#### 【0018】

このような構成において、オーディオサーバ 30がソース 10から出力されるデジタルオーディオデータを保存する場合には、そのデジタルオーディオデータは、入力インターフェイス回路 35を通じて暗号化回路 41に供給され、図 2に示すように暗号化される。

#### 【0019】

ここで、図 2Aは、暗号化回路 41に入力されるデジタルオーディオデータを示し、図 2Bは、暗号化回路 41から出力されるデジタルオーディオデータを示す。そして、暗号化回路 41の出力デジタルオーディオデータにおいては、斜線を付けた部分だけが暗号化されている。すなわち、暗号化回路 41においては、もとのデジタルオーディオデータのうち、所定の周期  $T$  ごとに、所定の期間  $\tau$  の部分（斜線部分）だけが暗号化される。この場合、値  $T$ 、 $\tau$  は、暗号化回路 41

の一部として、ROM 32 のプログラムに用意される。また、一例として、 $T = 23\text{ms}$ 、 $\tau = 1\text{ms}$ とされる。

#### 【0020】

そして、この部分的に暗号化されたデジタルオーディオデータが HDC 37 を通じて HDD 38 に書き込まれる。

#### 【0021】

一方、オーディオサーバ 30 に保存されているデジタルオーディオデータを使用する場合には、まず、認証回路 43 により出力装置 20 に対する認証処理が行われる。そして、その認証処理の結果、出力装置 30 が正当な出力装置のときには、HDC 37 を通じて HDD 38 から目的とするデジタルオーディオデータが読み出され、この読み出されたデジタルオーディオデータが復号化回路 42 に供給され、周期  $T$  ごとの期間  $\tau$  の暗号化部分が復号化されてもとのデジタルオーディオデータが取り出され、このデジタルオーディオデータが出力インターフェイス回路 36 を通じて出力装置 20 に供給され、音響として再生される。

#### 【0022】

なお、出力装置 20 に対する認証処理の結果、出力装置 30 が正当な出力装置ではないときには、HDD 38 からのデジタルオーディオデータの読み出しは行われず、したがって、出力装置 20 へのデジタルオーディオデータの出力は許可されない。

#### 【0023】

こうして、上述のオーディオサーバ 30 によれば、デジタルオーディオデータを保存し、これを必要なときに取り出すことができる。そして、その場合、オーディオサーバ 30 から HDD 38 を物理的に取り出してパーソナルコンピュータに接続することにより、HDD 38 に保存されているデジタルオーディオデータを他の HDD や CD-R などにコピーして再生することができる。

#### 【0024】

しかし、他の HDD や CD-R にコピーしたデジタルオーディオデータは、図 2B に示すように、周期  $T$  ごとの期間  $\tau$  の暗号化部分を有するとともに、この暗号化部分のデジタルオーディオデータは、パーソナルコンピュータにおいては復

号化されることなく音響として再生されるので、図2Cに示すように、その暗号化部分はノイズ音として出力される。

#### 【0025】

つまり、HDD38のデジタルオーディオデータを他のHDDやCD-Rなどにコピーしても、その再生音には周期的にノイズ音が含まれるので、音楽などの再生に支障をきたし、実用にならない。したがって、著作権者の権利を守ることができる。

#### 【0026】

しかも、CPU31が、暗号化回路41の暗号化処理および復号化回路42の復号化処理を実行するのは、周期Tごとに期間 $\tau$ であり、つまり、全体の $\tau/T$ の期間であるから、この割り合い $\tau/T$ および値 $\tau$ をあらかじめ小さくしておくことにより、暗号化処理および復号化処理に対するCPU31の負担を軽減することができる。したがって、CPU31として処理能力の高いものを必要しない。あるいはCPU31の処理能力が低くても、その暗号化処理および復号化処理を実行することができる。また、これにより、暗号化や復号化のために専用のICを設ける必要もない。したがって、オーディオサーバ30のコストを低減することができる。

#### 【0027】

図3は、この発明をCDおよびCDプレーヤに適用した場合の一例を示す。まず、CDの作製時（記録時）、アナログオーディオ信号L、RがA/Dコンバータ回路51に供給されてデジタルオーディオデータにA/D変換され、このデジタルオーディオデータが暗号化回路52に供給される。また、信号形成回路54から周期Tごとに期間 $\tau$ を示す信号が暗号化回路52に供給される。こうして、暗号化回路52において、これに供給されたデジタルオーディオデータは、図2Bに斜線で示すように、周期Tごとに期間 $\tau$ ずつ暗号化される。

#### 【0028】

そして、この部分的に暗号化されたデジタルオーディオデータが、記録回路53に供給されてエラー訂正のエンコードおよびEFM変調などの処理が行われ、このEFM信号がCDの原盤に記録される。なお、このとき、形成回路54から

値  $T$ 、 $\tau$  を示すデータが取り出され、このデータが暗号化回路 52 により暗号文データに暗号化されてから記録回路 53 に供給され、値  $T$ 、 $\tau$  の暗号文データが CD の原盤にサブコードとして記録される。こうして、図 2B に示すように部分的に暗号化されたデジタルオーディオデータを有する CD 60 が（その原盤から）作製される。

#### 【0029】

また、CD 60 の再生は CD プレーヤ 70 により行われる。すなわち、光学ピックアップ 71 により CD 60 から EFM 信号が再生され、この再生された EFM 信号が DSP 72 の再生回路 721 に供給される。この再生回路 721 および次段の復号化回路 722 は、DSP 72 が実行するプログラムにより実現されるものである。また、この DSP 72 には、この CD プレーヤ 70 の全体の動作などを制御するマイクロコンピュータ 80 が接続される。

#### 【0030】

そして、再生回路 721 において、記録回路 53 とは相補の処理が行われ、すなわち、EFM 信号の復調およびエラー訂正などが行われ、部分的に暗号化されたデジタルオーディオデータと、暗号化されたサブコードとが取り出され、そのデジタルオーディオデータが復号化回路 722 に供給される。また、再生回路 721 により取り出されたサブコードがマイクロコンピュータ 80 に供給され、CD 60 に対して、あらかじめ認証を受けているときには、もとの値  $T$ 、 $\tau$  のデータが復号化されて取り出され、この値  $T$ 、 $\tau$  のデータが復号化回路 722 に供給される。

#### 【0031】

そして、復号化回路 722 において、値  $T$ 、 $\tau$  を使用してデジタルオーディオデータの暗号化部分が復号化されてもとのデジタルオーディオデータとされる。そして、このデジタルオーディオデータが D/A コンバータ回路 73 に供給されてもとのアナログオーディオ信号  $L$ 、 $R$  に D/A 変換されて取り出される。

#### 【0032】

こうして、上述の CD 60 は、認証を受けた CD プレーヤ 70 で再生した場合には、正常に再生をすることができる。しかし、認証を受けていない CD プレー

やで再生した場合には、CD 60 から再生されたデジタルオーディオデータの暗号化部分が復号化されることなく音響として再生されるので、その暗号化部分はノイズ音として出力される。したがって、CD 60 を認証を受けていない CD プレーヤで再生した場合には、その再生に支障をきたし、実用にならないので、著作権者の権利を守ることができる。

#### 【0033】

しかも、DSP 72 が復号化回路 722 の復号化処理を実行するのは、全体の  $\tau/T$  の期間であるから、この割り合い  $\tau/T$  および値  $\tau$  をあらかじめ小さくしておくことにより、復号化処理に対する DSP 72 の負担を軽減することができ、DSP 72 として処理能力の高いものを必要しない。あるいは DSP 72 の処理能力が低くても、復号化処理を実行することができる。また、これにより、復号化のために専用の IC を設ける必要もない。したがって、CD プレーヤ 70 のコストを抑えることができる。

#### 【0034】

さらに、CD 60 の正規のユーザであれば、CD 60 を CD-R などにコピーしても再生をすることができるので、CD 60 のバックアップを取ることができる。

#### 【0035】

なお、上述において、オーディオサーバ 30 あるいは CD プレーヤ 70 が認証を受ける方法、あるいは暗号化部分を復号化するときに許可を受ける方法は、任意である。また、上述においては、デジタルオーディオデータが周期 T ごとに期間  $\tau$  ずつ暗号化部分を有する場合であるが、図 4 に示すように、デジタルオーディオデータに対して、任意の期間  $T_i$  ( $i=1\sim n$ ) ごとに、任意の期間  $\tau_i$  ずつ暗号化部分 (斜線図示) とすることもできる。特に、デジタルオーディオデータの内容が音楽の場合、期間  $T_i$  を数十小節のフレーズにしたり、期間  $\tau_i$  をサビの部分や音量の小さくなる部分に割り当てると効果的である。

#### 【0036】

そして、その場合には、図 1 のオーディオサーバ 30 であれば、値  $T_i$ 、 $\tau_i$  を例えば図 5 に示すようなテーブル (テーブルに相当するものを含む) の形式で R

OM32に用意し、あるいは図2のCDプレーヤ70であれば、そのテーブルをサブトラックに用意することができる。

#### 【0037】

また、図1のオーディオサーバ30においては、値 $T$ 、 $\tau$ （あるいは $T_i$ 、 $\tau_i$ ）をROM32に設けるとしたが、図2のCD60と同様、ソース10から得るようにすることもでき、その場合には、値 $T$ 、 $\tau$ を暗号化しておき、認証を受けたとき、その暗号化された値 $T$ 、 $\tau$ を復号化してデジタルオーディオデータの暗号化部分の復号化に使用することもできる。

#### 【0038】

さらに、上述においては、対象となるデジタルデータがデジタルオーディオデータの場合であるが、時間とともに連続的に変化する内容のデジタルデータであれば、ビデオ信号や動画などのデジタルデータであってもよい。また、HDD38の代わりに不揮発性メモリとすることもできる。

#### 【0039】

[この明細書で使用している略語の一覧]

A/D : Analog to Digital  
CD : Compact Disc  
CD-R : CD Recordable  
CPU : Central Processing Unit  
D/A : Digital to Analog  
DES : Data Encryption Standard  
DSP : Digital Signal Processor  
EFM : Eight to Fourteen Modulation  
HDC : Hard Disk Controller  
HDD : Hard Disk Drive  
IC : Integrated Circuit  
RAM : Random Access Memory  
ROM : Read Only Memory

#### 【0040】

**【発明の効果】**

この発明によれば、デジタルデータを保存したHDDを他のパーソナルコンピュータなどにより使用しても、デジタルデータは部分的に暗号化してあり、その暗号化部分はノイズとして再生されるので、実用的な再生とすることができず、著作権者の権利を守ることができる。

**【0041】**

しかも、その暗号化部分をあらかじめ小さくしておくことにより、再生に使用するCPUとして処理能力の高いものを必要しないとともに、復号化のために専用のICを設ける必要もないので、装置のコストを低減することができる。

**【図面の簡単な説明】****【図1】**

この発明の一形態を示す系統図である。

**【図2】**

この発明を説明するための図である。

**【図3】**

この発明の他の形態を示す系統図である。

**【図4】**

この発明を説明するための図である。

**【図5】**

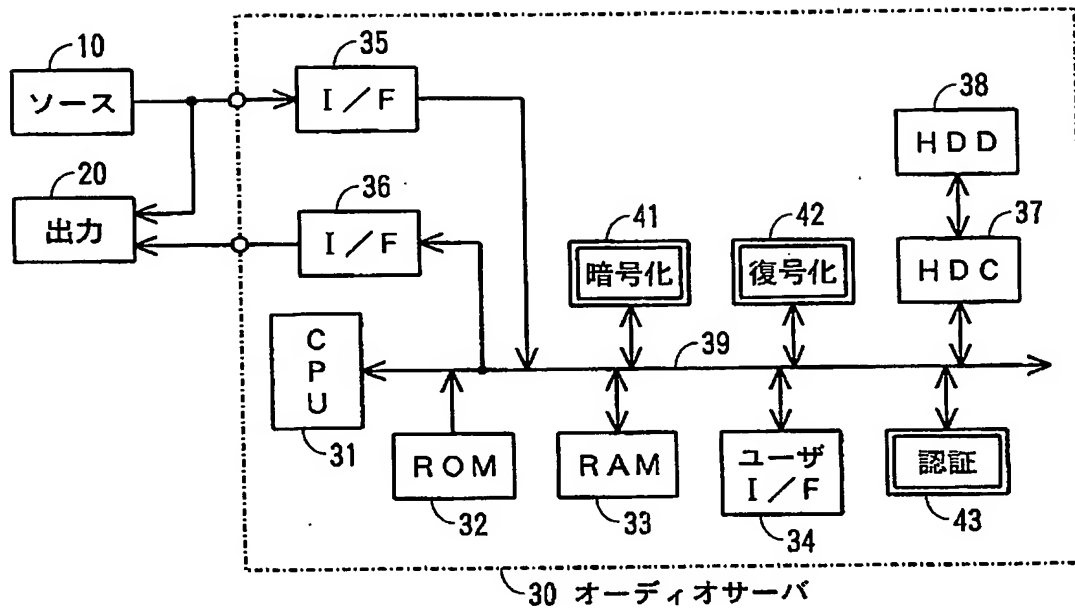
この発明を説明するための図である。

**【符号の説明】**

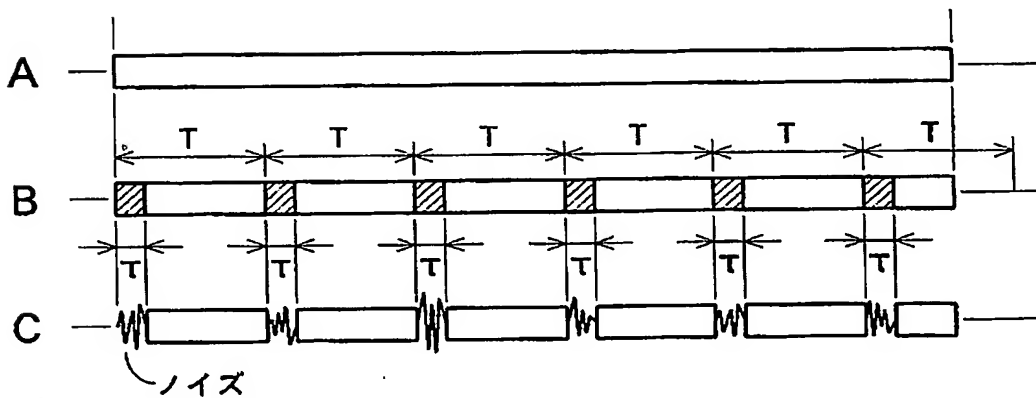
10…ソース、20…出力装置、30…オーディオサーバ、31…CPU、32…ROM、33…RAM、34…ユーザインターフェイス、35…入力インターフェイス、36…出力インターフェイス、37…HDC、38…HDD、39…システムバス、41…暗号化回路、42…復号化回路、43…認証回路

【書類名】 図面

【図 1】

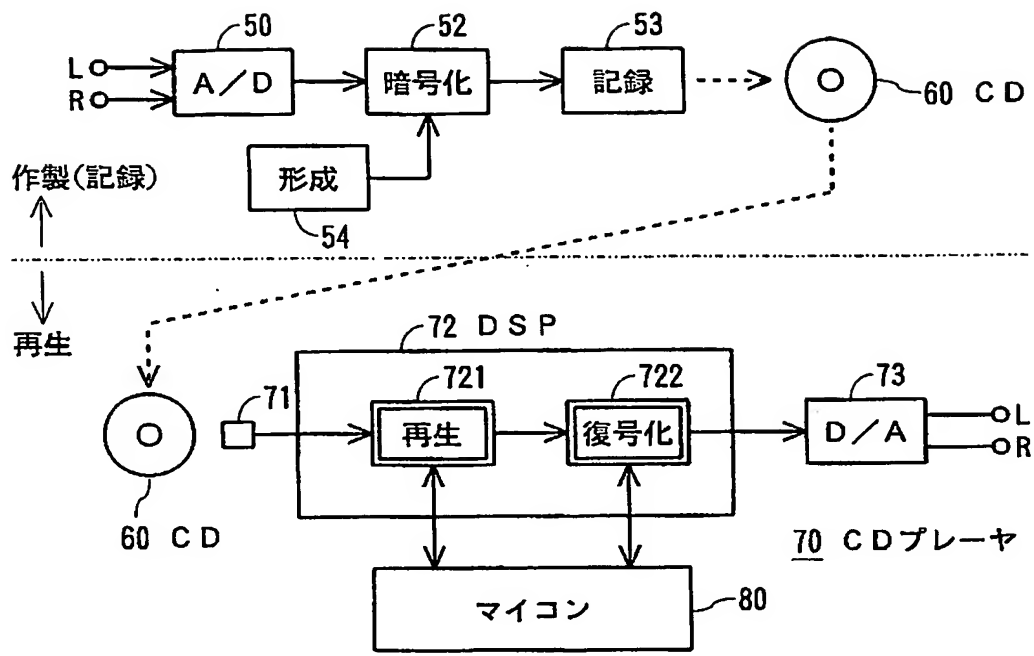


【図 2】

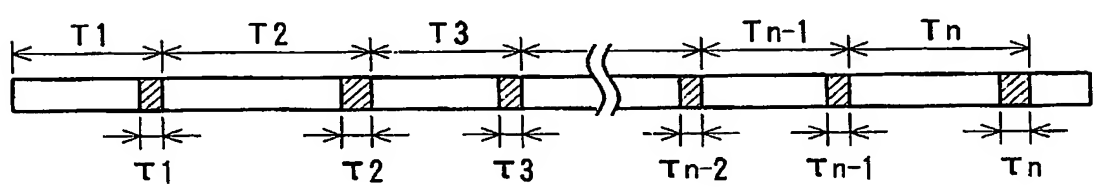




【図 3】



【図 4】



【図 5】

	期間(位置)	期間
暗号化部分 1	T1	τ1
暗号化部分 2	T2	τ2
暗号化部分 3	T3	τ3
⋮	⋮	⋮
暗号化部分 n	Tn	τn

【書類名】 要約書

【要約】

【課題】 デジタルオーディオデータやデジタルビデオデータなどのように、内容が時間とともに変化するデジタルデータに対して、不正なコピーや不正な再生を実質的に無効にする。

【解決手段】 内容が時間とともに変化するデジタルデータに対して、所定の時間  $T$  ごとに所定の期間  $\tau$  ずつ部分的に暗号化を行う（図 2 B の斜線部分）。このとき、暗号化部分の期間  $\tau$  の所定の時間  $T$  に対する割り合い、および暗号化部分の占める期間  $\tau$  が、十分に小さくなるように暗号化を行う。この暗号化のされたデジタルデータを保存する。

【選択図】 図 2

特願 2 0 0 3 - 1 0 7 2 7 8

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 2 1 8 5 ]

1. 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都品川区北品川 6 丁目 7 番 3 5 号

氏 名

ソニー株式会社